

UNIVERSITAS BINA NUSANTARA

Jurusan Teknik Informatika
Skripsi Sarjana Komputer
Semester Ganjil Tahun 2005/2006

ANALISIS DAN PERANCANGAN VPN PADA KONEKSI KANTOR CABANG DAN MOBILE USER DENGAN KANTOR PUSAT PT. ANGKASA PURA II

Eka Gunawan	0600613836
Teddy Herryanto	0600662586
William Hartoyo	0600670184

Kelas / Kelompok : 07PAT / 01

Abstrak

Saat ini sudah banyak sekali perusahaan yang mempunyai banyak cabang menggunakan jasa internet dengan teknologi yang ditawarkan oleh *provider* internet dengan jenis dan harga yang bervariasi untuk memenuhi kebutuhan komunikasi perusahaan. Namun, masih banyak yang menggunakan *dial-up* privat dari cabang ke pusat. Sistem ini lebih mengeluarkan biaya yang besar setiap koneksinya. Adapun tujuan penelitian ini adalah untuk merancang suatu jaringan yang ekonomis dalam hal biaya koneksi dan menjamin keamanan pertukaran data antara pusat dan cabang. Metode yang dipilih dan dilakukan adalah menganalisis kebutuhan dan sistem berjalan (*bandwidth*, biaya, koneksi pusat dan cabang), merancang IPSec, konfigurasi router pusat dan cabang serta radius server untuk *mobile user*. Pengujian juga akan kami lakukan untuk membandingkan hasil dari sistem yang diusulkan dengan sistem berjalan. Hasil yang diharapkan adalah menciptakan sistem dengan biaya koneksi yang cukup ekonomis dan faktor keamanan yang memadai antara kantor pusat dan cabang sehingga kantor cabang tidak perlu mengeluarkan biaya koneksi yang tinggi. Pada kasus ini, misalkan kantor cabang di Medan tidak harus *dial-up* ke Jakarta atau *mobile users* tidak perlu mengeluarkan biaya SLJJ (Sambungan Langsung Jarak Jauh) atau internasional di mana pun mereka berada. Tentunya bukan saja biaya koneksi yang mengalami penghematan, keamanan transaksi data pun menjadi fasilitas yang akan didapat dengan VPN (*Virtual Private Network*) yang dirancang dan diusulkan. Simpulan yang didapatkan adalah data transaksi dari cabang atau *mobile user* ke pusat akan dienkripsi untuk menjamin keamanan data dan jalur komunikasi tidak lagi menggunakan *dial-up private* sehingga biaya komunikasi akan jauh lebih hemat.

Kata kunci : VPN, koneksi, *mobile user*

KATA PENGANTAR

Puji dan syukur kami panjatkan kepada Tuhan Yang Maha Esa atas segala berkat dan kekuatan yang diberikan-Nya kepada penulis, sehingga dapat menyelesaikan penulisan skripsi kami yang berjudul "Analisis dan Perancangan VPN pada Koneksi Kantor Cabang ke Kantor Pusat PT. Angkasa Pura II". Skripsi ini merupakan karya ilmiah yang disusun sebagai salah satu syarat kelulusan dalam jenjang pendidikan S1 (Strata Satu) jurusan Teknik Informatika di Universitas Bina Nusantara, Jakarta.

Dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah membimbing, memberikan petunjuk, saran, nasehat dan bantuan baik moril maupun materiil. Adapun pihak-pihak tersebut yaitu:

1. Bapak Prof. Dr. Gerardus Polla, M.App.Sc. selaku Rektor Universitas Bina Nusantara yang memberikan kesempatan untuk menimba ilmu di Universitas Bina Nusantara
2. Bapak Mohammad Subekti, BE, M.Sc. selaku Ketua Jurusan Teknik Informatika Universitas Bina Nusantara
3. Bapak Fredy Purnomo, S.Kom., M.Kom. selaku Sekretaris Jurusan Teknik Informatika Universitas Bina Nusantara
4. Bapak Rusdianto Roestam, Ir., M.sc, Ph.D selaku Dosen Pembimbing yang telah memberikan bimbingan dan pengarahan yang sangat membantu dalam penyusunan skripsi ini

5. Bapak Eduardus Rumyaan, S.Kom selaku ISS Manager, Bapak Hermawan, S.Kom dan Bapak Wasiman, S.Kom selaku Asisten Manager, Bapak Hartono, Bapak Subowo, Salman Husni, Eddy Putranto dan Bapak M. Ikhsan selaku staff ISS dan seluruh jajaran staff PT. Angkasa Pura II yang turut memberikan kesempatan dan kemudahan administrasi
6. Orangtua dan sahabat-sahabat kami yang telah memberikan dukungan baik dalam bentuk moril dan materiil.

Akhir kata, penulis berharap agar skripsi ini dapat bermanfaat bagi pembaca dan dapat dijadikan sebagai masukan pemikiran untuk perkembangan ilmu komputer khususnya dan dunia pendidikan pada umumnya.

Jakarta, Januari 2005

Penulis

DAFTAR ISI

Halaman Judul Luar.....	i
Halaman Judul Dalam.....	ii
Halaman Persetujuan <i>Hardcover</i>	iii
Halaman Pernyataan Dewan Penguji.....	iv
ABSTRAK.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xvi
DAFTAR GAMBAR.....	xvii
BAB 1 : PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Ruang Lingkup.....	4
1.3 Tujuan dan Manfaat	4
1.4 Metodologi.....	5
1.5 Sistematika Penulisan	8
BAB 2 : LANDASAN TEORI	10
2.1 Jaringan Komunikasi Data.....	10
2.1.1 Model OSI Layer	10
2.1.1.1 Layer 1 : <i>Physical Layer</i>	11

2.1.1.2	Layer 2 : <i>Data Link Layer</i>	12
2.1.1.3	Layer 3 : <i>Network Layer</i>	12
2.1.1.4	Layer 4 : <i>Transport Layer</i>	12
2.1.1.5	Layer 5 : <i>Session Layer</i>	12
2.1.1.6	Layer 6 : <i>Presentation Layer</i>	13
2.1.1.7	Layer 7 : <i>Application Layer</i>	13
2.1.2	Model TCP / IP	13
2.1.2.1	<i>Application Layer</i>	14
2.1.2.2	<i>Transport Layer</i>	15
2.1.2.3	<i>Internet Layer</i>	15
2.1.2.4	<i>Network Access Layer</i>	17
2.2	Klasifikasi Jaringan.....	17
2.2.1	<i>Local Area Network (LAN)</i>	17
2.2.1.1	Topologi LAN.....	17
2.2.1.2	Protokol LAN.....	18
2.2.2	<i>Metropolitan Area Network (MAN)</i>	19
2.2.3	<i>Wide Area Network (WAN)</i>	20
2.2.3.1	Topologi WAN	20
2.2.3.2	Protokol WAN	21
2.3	IP Address	21
2.3.1	Kelas – Kelas IP Address	22
2.3.2	<i>Private IP Address</i>	23

2.4	<i>Virtual Private Network (VPN)</i>	23
2.4.1	<i>Tipe VPN</i>	25
2.4.1.1	<i>Site-to-Site VPN</i>	25
2.4.1.2	<i>Extranet VPN</i>	25
2.4.1.3	<i>Remote Access VPN</i>	26
2.4.2	<i>Topologi VPN</i>	27
2.4.2.1	<i>Topologi Hub dan Spoke</i>	27
2.4.2.1	<i>Topologi Partial atau Full Mesh</i>	28
2.4.2.1	<i>Topologi Hybrid</i>	29
2.5	<i>Tunneling</i>	30
2.5.1	<i>Peranan Tunneling</i>	31
2.5.2	<i>Arsitektur IP Tunneling VPN</i>	32
2.5.2.1	<i>IPSec Tunneling dan Encryption</i>	33
2.5.2.2	<i>GRE Tunneling</i>	34
2.6	<i>IPSec</i>	35
2.6.1	<i>Encryption</i>	35
2.6.1.1	<i>Symmetrical Key Encryption</i>	36
2.6.1.1	<i>Asymmetrical Key Encryption</i>	37
2.6.2	<i>Authentication</i>	38
2.6.2.1	<i>User Authentication</i>	38
2.6.2.1	<i>Data Authentication</i>	39
2.6.3	<i>IPSec Mode</i>	40
2.6.3.1	<i>IPSec Transport Mode</i>	40

2.6.3.2	IPSec <i>Tunnel Mode</i>	41
2.6.4	IPSec <i>Security Protocol</i>	42
2.6.4.1	<i>Authentication Header</i> (AH).....	43
2.5.2.1	<i>Encapsulating Security Payload</i> (ESP)	44
2.6.5	<i>Security Association dan Key Management</i>	46
2.7	RADIUS (<i>Remote Authentication Dial-in User Services</i>).....	48
BAB 3 : ANALISIS SISTEM BERJALAN		49
3.1	Profil Perusahaan PT. Angkasa Pura II	49
3.1.1	Visi dan Misi.....	50
3.1.2	Pelayanan Angkasa Pura II	50
3.1.2.1	Jasa Aeronautika	50
3.1.2.2	Jasa Non Aeronautika	51
3.1.3	Sumber Daya Manusia yang Kompeten	52
3.1.4	Peran Sosial Kemasyarakatan	53
3.1.5	Alisansi Perusahaan	53
3.1.4.1	PT. Gapura Angkasa	54
3.1.4.2	PT. Angkasa Pura Schipol	54
3.1.4.3	PT. Purantara Mitra Angkasa Dua	54
3.2	Struktur Organisasi	55
3.2.1	Pembagian Tugas dan Tanggung Jawab	56
3.3	Koneksi Jaringan yang Sedang Berjalan.....	59
3.3.1	Jaringan Lokal (LAN).....	61

3.3.2	Jaringan Koneksi Akses Internet.....	64
3.3.3	Koneksi Kantor Cabang.....	67
3.3.4	Analisis Penggunaan <i>Bandwidth</i>	69
3.3.4.1	Penggunaan <i>Bandwidth</i> pada Kantor Pusat	69
3.3.4.2	Penggunaan <i>Bandwidth</i> pada Kantor Cabang.....	70
3.4	Permasalahan	71
3.5	Usulan Pemecahan Masalah	72
BAB 4 : USULAN SOLUSI RANCANGAN dan KONFIGURASI.....		75
4.1	Usulan Rancangan Koneksi Kantor Cabang.....	75
4.1.1	Analisis Perbandingan <i>Transfer Rate</i>	77
4.1.2	Analisis Perbandingan Biaya Koneksi Kantor Cabang	79
4.1.2.1	Analisis Biaya Sistem Berjalan.....	79
4.1.2.2	Analisis Biaya Sistem Usulan	81
4.2	Usulan Koneksi <i>Mobile User</i>	82
4.2.1	Analisa Perbandingan Biaya Koneksi <i>Mobile User</i>	83
4.3	Pemilihan <i>Software</i> dan <i>Hardware</i> yang Akan Digunakan.....	84
4.4	Usulan Solusi Perancangan VPN.....	85
4.4.1	<i>Site-to-Site</i> VPN.....	88
4.4.2	<i>Remote Access</i> VPN.....	95
4.4.2.1	Konfigurasi RADIUS.....	99
4.4.2.2	Konfigurasi Cisco VPN Client.....	103

4.5	Usulan Konfigurasi VPN	108
4.5.1	Konfigurasi <i>Site-to-Site</i> VPN.....	108
4.5.1.1	Konfigurasi VPN Kantor Pusat AP II.....	108
4.5.1.2	Konfigurasi VPN Kantor Cabang AP II	113
4.5.2	Konfigurasi <i>Remote Access</i> VPN.....	115
4.6	Evaluasi VPN.....	117
4.6.1	<i>Testing</i> VPN.....	117
4.6.2	Keuntungan dan Kelemahan VPN	120
4.6.2.1	Keuntungan VPN	120
4.6.2.2	Kelemahan VPN	123
BAB 5 : SIMPULAN dan SARAN		125
5.1	Simpulan	125
5.2	Saran	126
DAFTAR PUSTAKA		127
RIWAYAT HIDUP		128
LAMPIRAN - LAMPIRAN		
FOTOCOPY SURAT SURVEI		

DAFTAR TABEL

Tabel 2.1 Kelas – kelas IP <i>address</i>	22
Tabel 2.2 Kelompok private IP <i>address</i>	23
Tabel 3.1 Sever <i>dial-up</i> privat vs <i>dial-up</i> via ISP.....	73
Tabel 4.1 Biaya Koneksi Kantor Cabang	80
Tabel 4.2 Biaya Koneksi Internet	81
Tabel 4.3 Total Biaya Sistem Berjalan	81
Tabel 4.4 Total Biaya Sistem Usulan	82
Tabel 4.5 Perbandingan <i>Dial-up</i> ISP dan <i>Dial-up</i> Privat untuk <i>Mobile User</i>	84
Tabel 4.6 Rancangan Koneksi Router Kantor Pusat.....	86
Tabel 4.7 Rancangan <i>Access List</i> Router Kantor Pusat	87
Tabel 4.8 Rancangan Koneksi Router Kantor Cabang	88
Tabel 4.9 Perancangan GRE Tunnel.....	91
Tabel 4.10 Tabel <i>Routing</i>	92
Tabel 4.11 Rancangan ISAKMP <i>Policy</i>	93
Tabel 4.12 Perancangan VPN Kantor Pusat dengan Halim Perdanakusuma	94
Tabel 4.13 Perancangan VPN untuk <i>Mobile User</i>	99
Tabel 4.14 Perancangan Koneksi RADIUS.....	100

DAFTAR GAMBAR

Gambar 2.1 <i>Seven Osi Layer</i>	11
Gambar 2.2 Model TCP/IP	14
Gambar 2.3 Topologi – topologi LAN	18
Gambar 2.4 LAN, MAN dan WAN.....	19
Gambar 2.5 Topologi <i>Tiered</i>	20
Gambar 2.6 <i>Virtual Private Networking (VPN)</i>	24
Gambar 2.7 <i>Site-to-Site VPN</i>	25
Gambar 2.8 <i>Extranet VPN</i>	26
Gambar 2.9 <i>Remote Access VPN</i>	27
Gambar 2.10 Topologi <i>hub</i> dan <i>spoke</i>	28
Gambar 2.11 Topologi <i>partial mesh</i>	29
Gambar 2.12 Topologi <i>hybrid</i>	30
Gambar 2.13 <i>Tunneling</i>	31
Gambar 2.14 VPN menggunakan <i>IPSec Tunneling</i>	33
Gambar 2.15 <i>Symmetrical Key Encryption</i>	37
Gambar 2.16 <i>Asymmetrical Key Encryption</i>	38
Gambar 2.17 Paket IP dalam <i>IPSec Transport Mode</i>	41
Gambar 2.18 Paket IP dalam <i>IPSec Tunnel Mode</i>	42
Gambar 2.19 Paket IP yang diproteksi dengan AH	43
Gambar 2.20 Paket IP yang diproteksi dengan AH dalam <i>transport mode</i>	44
Gambar 2.21 Paket IP yang diproteksi dengan AH dalam <i>tunnel mode</i>	44

Gambar 2.22 Paket IP yang diproteksi dengan ESP	45
Gambar 2.23 Paket IP yang diproteksi dengan ESP dalam <i>transport mode</i>	45
Gambar 2.24 Paket IP yang diproteksi dengan ESP dalam <i>tunnel mode</i>	46
Gambar 3.1 Struktur Organisasi PT. Angkasa Pura II.....	55
Gambar 3.2 Jaringan pada PT. Angkasa Pura II.....	60
Gambar 3.3 Koneksi antar PC per-tiap lantai pada LAN	61
Gambar 3.4 <i>Server Farm</i>	63
Gambar 3.5 <i>Backbone</i> jaringan lokal.....	64
Gambar 3.6 Koneksi Akses Internet	65
Gambar 3.7 Koneksi <i>dial-up</i> dari kantor cabang / <i>mobile user</i> ke kantor pusat.....	68
Gambar 3.8 Penggunaan <i>bandwidth</i> per hari pada Kantor Pusat AP II.....	70
Gambar 3.9 Penggunaan <i>bandwidth</i> per hari pada Kantor Cabang Palembang	70
Gambar 3.10 Penggunaan <i>bandwidth</i> per hari pada Kantor Cabang Medan.....	71
Gambar 4.1 Usulan solusi koneksi kantor cabang dan <i>mobile user</i>	76
Gambar 4.2 <i>Download</i> data dengan <i>dial-up</i>	78
Gambar 4.3 <i>Download</i> data dengan <i>dedicated</i> internet	78
Gambar 4.4 Usulan solusi koneksi <i>mobile user</i>	83
Gambar 4.5 Membuat user pada RADIUS	100
Gambar 4.6 Penentuan <i>password</i> untuk user pada RADIUS	101
Gambar 4.7 Setting AAA Client pada RADIUS	101
Gambar 4.8 Konfigurasi network pada RADIUS	102
Gambar 4.9 Setting Log pada RADIUS	102
Gambar 4.10 Cisco VPN Client.....	103

Gambar 4.11 Penentuan nama koneksi pada Cisco VPN Client	104
Gambar 4.12 Penentuan IP address pada Cisco VPN Client	104
Gambar 4.13 Penentuan group pada Cisco VPN Client	105
Gambar 4.14 Melakukan koneksi pada Cisco VPN Client	105
Gambar 4.15 Inisialisasi koneksi Cisco VPN Client	106
Gambar 4.16 Authentikasi pada Cisco VPN Client	106
Gambar 4.17 Status koneksi Cisco VPN Client	107
Gambar 4.18 Statistik koneksi Cisco VPN Client	107
Gambar 4.19 Sniff paket data tanpa VPN	119
Gambar 4.20 Sniff paket data dengan VPN	119